

Amendments To the Claims:

1-7. (canceled)

8. (currently amended) An automation network comprising:

a first subnetwork comprising a first plurality of subscribers;

a second subnetwork comprising a second plurality of subscribers including one or more process devices not configured to provide an end point of a secure tunnel, the second plurality of subscribers including process devices taken from the group consisting of an automation device, a measurement transducer, an operating and monitoring device and a programming device;

the network arranged to provide secure data transfer between a first subscriber or multiple ones of the subscribers arranged in the first sub-network and a second subscriber or multiple ones of the subscribers arranged in the second sub-network,

with the first subnetwork comprising at least a first secure-switch connected upstream of the first subscriber or the multiple ones of the subscribers arranged in the first subnetwork,

with the second subnetwork comprising at least a second secure-switch connected upstream of at least one process device not capable of producing a tunnel end point,

with the first and second secure switches configured for establishing a secure tunnel having two end points, the first end point being in the first secure switch and the second end point being in the second secure switch, the tunnel configured between the first and second subnetworks to securely transmit data via an insecure network, wherein a point-to-point connection is made between the first subscriber of the first subnetwork and the at least one process device not capable of producing a tunnel end point in the second subnetwork;

the first secure-switch is an Ethernet switch and at least one port of the tunnel is a layer-3-port for establishing a tunnel end point in accordance with the Ipsec-protocol, and

wherein, in addition to the first secure switch being configured to establish the secure tunnel for at least the first subscriber the connection is made using a subscriber address of the first subscriber.

9. (previously presented) The arrangement according to claim 8, further comprising a configuration tool for configuring the automation network, the configuration tool configured to generate parameter data related to the secure-switch and to automatically transmit the generated data to the secure-switch.

10. (previously presented) The arrangement according to claim 8, wherein the secure-switch comprises at least one port configured as a WLAN end point for establishing a tunnel end point.

11. (previously presented) The arrangement according to claim 8, wherein the secure-switch comprises at least one port configured to be used as a tunnel end point, the at least one point having a marker.

12. (previously presented) The arrangement according to claim 11, wherein the marker is switchable.

13. (previously presented) A secure-switch for securing data access of a first subscriber or a plurality of first subscribers arranged in a first sub-network of an automation network to a second subscriber or a plurality of second subscribers arranged in a second sub-network of the automation network, wherein

the secure switch is configured to be connected upstream of the first subscriber or the plurality of first subscribers, and

the secure switch is an Ethernet switch having at least one port embodied as a layer-3-port for establishing a first tunnel end point in accordance with the IPsec protocol,

the secure switch comprising a secure channel converter for establishing a tunnel to a second secure switch connected upstream of the second subscriber or the plurality of second subscribers, the second secure switch being an Ethernet switch having at least one port embodied as a layer-3-port for establishing a second tunnel end point in accordance with the IPsec protocol, the first and second tunnel endpoints defining a tunnel configured to securely transmit data via an insecure network, wherein the secure channel converter is configured to establish the tunnel representative for the first subscriber or the plurality of first subscribers and to allocate the tunnel to the first subscriber or the plurality of first subscribers using a subscriber address of the first subscriber or the plurality of first subscribers, thereby effecting, in combination with the second secure switch, a point-to-point connection between at least the first subscriber and the second subscriber.

14. (previously presented) The network of claim 8 wherein, in addition to the secure switch being configured to establish the secure tunnel for at least the first subscriber, the connection is made using a subscriber address of the first subscriber and an address allocated to the at least one process device not capable of producing a tunnel end point in the second subnetwork, thereby effecting the point-to-point connection.

Serial No. 10/564,211  
Atty. Doc. No. 2003P05103WOUS

15. (previously presented) The secure-switch of claim 13 further including a secure port, a plurality of non-secure ports, and a switch matrix, with the secure channel converter positioned between the secure port and the switch matrix and with the switch matrix positioned between the secure channel converter and the non-secure ports, so that all data passing through the secure port and into the secure switch pass through the secure channel converter before reaching an unsecured port.